United States General Accounting Office

GAO

Report to the Secretary of Defense

August 1999

DOD INFORMATION SECURITY

Serious Weaknesses Continue to Place Defense Operations at Risk

G A O

Accountability * Integrity * Reliability

GAO/AIMD-99-107

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-282190

August 26, 1999

The Honorable William S. Cohen
The Secretary of Defense

Dear Mr. Secretary:

The Department of Defense (DOD) relies on a vast and complex information infrastructure to support critical operations such as designing weapons, identifying and tracking enemy targets, paying soldiers, mobilizing reservists, and managing supplies. Indeed, its warfighting capability depends upon computer-based telecommunications networks and information systems. In recent years, numerous internal and external evaluations have identified weaknesses in information security that could seriously jeopardize DOD's operations and compromise the confidentiality, integrity, or availability of sensitive information. This report summarizes the results of our latest review of information security at DOD.

In May 1996, we reported that external attacks on DOD computer systems were a serious and growing threat.[1] According to DOD officials, attackers had stolen, modified, and destroyed both data and software. They had installed "back doors" that circumvented normal system protection and allowed attackers unauthorized future access. They had shut down and crashed entire systems and networks.

In September 1996, we issued a report, based on detailed analyses and testing of general computer controls, that identified pervasive vulnerabilities in DOD information systems.[2] We had found that authorized users could also exploit the same vulnerabilities that made external attacks possible to commit fraud or other improper or malicious acts. In fact,

[1] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

[2] **General computer controls** are the policies and procedures that affect the overall security and effectiveness of computer systems and operations, as opposed to being unique to any specific computer program, office, or operation. General controls include the organizational structure, operating procedures, software security features, and physical protection designed to ensure that (1) access to computer systems and sensitive data is restricted to prevent unauthorized changes and disclosure, (2) only approved changes are made to computer programs, (3) back-up and recovery plans are adequate to continue essential operations in the event of an emergency, and (4) computer staff duties are properly segregated to reduce the risk of undetected errors or fraud.

knowledgeable insiders with malicious intentions could pose a more serious threat than outsiders since they may be more aware of system weaknesses and how to disguise inappropriate actions. Our report highlighted the lack of a comprehensive information security program and made numerous recommendations for corrective actions.[3]

Subsequent reviews of individual systems also have disclosed serious weaknesses in information security. For example, we reported in 1997 that our review of the actuarial application supporting DOD's Military Retirement Trust Fund disclosed a lack of overall security administration and management governing access to Fund data files and other files storing sensitive information, such as social security numbers, pay rates, child and spousal abuse allegations, and medical test results.[4] In another example, two cases in which employees embezzled nearly $1 million led to our 1998 review of Air Force's vendor payment system. We identified a number of internal control weaknesses, including information security weaknesses, which leave the Air Force vulnerable to similar thefts.[5]

Tests conducted by the Joint Chiefs of Staff during the summer of 1997 demonstrated the continuing vulnerability of DOD and civilian networks to attack. Since then, DOD has acknowledged that it has continued to identify organized intrusions, indicating that such activities are an ongoing problem.

Because of the risks that inadequate information security poses to DOD operations and the integrity of its data, we followed up on our previous reviews of DOD's general computer controls.[6] Our objective was to provide an update on the status of corrective actions DOD has taken to (1) address specific weaknesses identified in our 1996 reports, in particular the September 1996 report and (2) develop a comprehensive departmentwide information security program.

[3]This report was designated Limited Official Use because of the sensitive information it contained.

[4]Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997).

[5]Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/AIMD-98-274, September 28, 1998).

[6]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996) and the September 1996 Limited Official Use report.

Results in Brief

Serious weaknesses in DOD information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data. These weaknesses impair DOD's ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its systems is properly authorized, tested, and functioning as intended, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks or fraud.

Our current review found that some corrective actions have been initiated in response to the recommendations our 1996 reports made to address pervasive information security weaknesses in DOD. However, progress in correcting the specific control weaknesses identified during our previous reviews has been inconsistent across the various DOD components involved and weaknesses persist in every area of general controls. Accordingly, we reaffirm the recommendations made in our 1996 reports. The status of DOD actions to implement those recommendations is discussed later in this report.

The DOD component activities we evaluated generally did not have effective processes for identifying and resolving information security weaknesses. However, the Defense Information Systems Agency (DISA),[7] which operates the Defense Megacenters (DMC), has established and is implementing a comprehensive security review process. DISA developed Standard Technical Implementation Guides (STIG), which prescribe clear and detailed standards for configuring its system software.[8] Also, DISA's Security Readiness Review (SRR) process enables it to test DMC compliance with the STIGs and other DISA security standards, track the weaknesses identified by the testing, and monitor and report on efforts to

[7]DISA is a major provider of telecommunications and computing services, supporting the military services and other Defense agencies on a fee-for-service basis. The Defense Services and other Defense agencies, however, continue to perform some data processing outside of the DMCs in data processing centers that are not subject to DISA's security review process.

[8]**System software** includes operating systems, utility software, program library systems, file maintenance software, security software, data communications systems, and database management systems. One set of system software may be used to support and control a number of user applications.

correct them. Thus far, DISA has identified and resolved thousands of security weaknesses.

At the end of our review, however, DISA was still developing guidance for configuring some of its system software and had not yet reviewed security over all of its systems. Moreover, some ongoing weaknesses were improperly reported as having been corrected because DISA has not always independently verified in a timely manner the corrective actions reported by its DMCs.

To provide a comprehensive, departmentwide information security program, which our September 1996 report recommended, DOD announced in January 1998 its plans for a Defense-wide Information Assurance Program (DIAP)[9] under the jurisdiction of the DOD Chief Information Officer (CIO). In February 1999, DOD's CIO finalized the Implementation Plan for the DIAP that outlines organizational structure and responsibilities. The program is still being staffed; DIAP staff will be responsible for creating a DIAP concept of operations to address the program's operational structure and processes.

In December 1998, DOD also implemented the Joint Task Force for Computer Network Defense, which DOD expects will support the DIAP by monitoring DOD's computer networks and defending against hacker attacks and other unauthorized access. DISA's security oversight program and other models for information security management offer approaches that DOD could adapt and integrate into its departmentwide program to address threats to information security not covered by the Joint Task Force. Because DIAP and task force efforts are at an early stage of development, their ultimate effectiveness cannot yet be assessed.

In order that the full potential of DISA's security oversight program, the DIAP, and other DOD IA initiatives can be realized, we are recommending that (1) the SRR process be expanded to include timely and independent verification of the corrective actions reported by DMCs and (2) the DIAP define how its efforts will be coordinated with the Joint Task Force and other related initiatives.

[9]DOD defines **information assurance** as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes capabilities to protect against, detect, and react to attacks.

In commenting on a draft of this report, DOD officials stated that they generally concurred with the report and its recommendations. They said that this report adds credence to efforts to heighten awareness within the DOD community of the serious risks that accompany poor security practices in information systems. They noted that DOD is actively working to correct the deficiencies cited in the report and they believe it is making progress in reducing the risks to its information systems.

Background

The DOD information processing environment is large, complex, and decentralized. DOD has over 2.1 million computers, over 10,000 local area networks, and over 100 long-distance networks. Its tens of thousands of automated information systems run on a variety of systems, including mainframe, mid-tier, client-server, and personal computer-based systems.

Security over these systems involves a number of functional areas. These include groups and individuals who use and own these systems, application developers, data center personnel (such as systems programmers, computer operators, and security managers), and others who come in contact with computer resources or data.

The owners of application systems and data are those organizations or individuals responsible for specifying the level of security required for their operations and supporting information systems, determining who is given access to their computer applications, prioritizing critical application programs to be covered by disaster recovery plans, and protecting their own system passwords and equipment. Application developers are responsible for managing software application program changes, ensuring the integrity of the application, and designing security controls within these applications consistent with owner requirements. Data center personnel are responsible for computer operations, system software configuration and change management, controls over access to data and programs at the system level, and some aspects of disaster recovery. Managers of the facilities in which these activities take place are generally responsible to some extent for physical and environmental security.

In DOD, responsibility for the security of an individual application, such as a payroll system or weapon system, and its related data, is typically shared by several organizations. Any DOD component may be the owner or user of an application. Application development may be done in-house by the user's organization or by a central design activity (CDA) on a fee-for-service basis. All of the military services and many of the Defense agencies,

including the Defense Finance and Accounting Service (DFAS) and the Defense Logistics Agency (DLA), have CDA components. DISA, through its DMCs, is a major provider of data processing services for DOD. However, data processing services may be provided by the military services and other DOD components or by a non-DOD service provider. Any of these DOD components may be a tenant on an installation owned or managed by another DOD component or government agency. In DISA's case, for example, each DMC shares the responsibility for physical security with the host activity of the installation on which it is located.

In DOD, not all responsibilities are clearly assigned, however. For example, while the data center is responsible for the security of the system software and the developer for application security, neither has explicit responsibility for the security and integrity of the interfaces between operating systems and applications.

Objectives, Scope, and Methodology

To determine the extent to which specific information security weaknesses identified in our September 1996 report had been corrected, we tested the effectiveness of corrective actions taken. Our testing was carried out in four DMCs, three CDAs, and two customer (i.e., end-user) activities.[10] Our original review was an assessment of general computer controls, which affect the overall security and effectiveness of an organization's computer systems and operations rather than being unique to a particular computer program, office, or operation. Our tests of corrective actions were limited to those areas in which we had previously documented specific weaknesses. We did not test controls that we had previously found to be operating effectively. Our audit program was based on our Federal Information System Controls Audit Manual.[11]

We also evaluated DISA's processes for overseeing security in the DMCs. We compared the scope and content of their Security Technical Implementation Guides (STIG) for system software with each other and with external guidance. We documented their Security Readiness Review (SRR) process and its history, assessed the security of the SRR database,

[10]We are not identifying the specific activities and installations in which our testing was conducted because of the sensitive nature of our findings. These were generally the same activities in which our original testing was conducted, although due to organizational changes, the unit responsible for a particular computer control had in some cases changed.

[11]GAO/AIMD-12.19.6, January 1999.

and quantified the results of SRRs performed to date. We also gathered evidence about the reliability of the SRR database by testing selected controls that were reported as SRR findings and subsequently reported as fixed.

For assistance in testing corrective actions and evaluating DISA's processes for overseeing security, we contracted with PricewaterhouseCoopers LLP. We determined the scope of the contractor's audit work, monitored its progress, and reviewed the related workpapers to ensure that the resulting findings were adequately supported.

To determine the extent to which DOD had developed and implemented a departmentwide information security program, we examined the management and the implementation plans for the Defense-wide Information Assurance Program and monitored Defense's progress through the end of our fieldwork. We also received briefings on the new Joint Task Force for Computer Network Defense and interviewed DOD officials to learn about departmentwide initiatives related to our recommendations.

At each test location, we briefed management on the results of our fieldwork at that location. We also briefed DOD officials on the results of our fieldwork at all locations. We requested comments on a draft of this report from the Secretary of Defense or his designee. On July 16, officials of the Infrastructure and Information Assurance Directorate of the Office of the Secretary of Defense provided us with oral comments that are discussed in the "Agency Comments and Our Evaluation" section of our report. Our work was performed from October 1997 through February 1999 in accordance with generally accepted government auditing standards.

Limited Progress in Correcting General Control Weaknesses

Our 1996 reports identified pervasive information security weaknesses in DOD and made recommendations for correcting them. While some corrective actions had been initiated to address our recommendations, our current review found that weaknesses persisted in every area of general controls.

Among the DOD components evaluated, only DISA had begun to establish a comprehensive process to identify and resolve information security weaknesses. DISA was issuing technical guidance to establish minimum standards for configuring system software and was implementing systematic entitywide inspections to monitor the effectiveness of computer

controls. As a result, DISA had identified and resolved thousands of control weaknesses.

Control Weaknesses Persist

In our current review we found that significant DOD information security weaknesses in general computer controls persisted for all the components evaluated, including DISA. The following sections give examples illustrating the types of weaknesses we found in access controls, application software development and change controls, segregation of duties, system software controls, and service continuity controls.

Access Controls

Access controls limit or detect inappropriate access to computer data, programs, facilities, and equipment to protect these resources against unauthorized modification, disclosure, loss, or impairment. Access controls include physical protections, such as gates and guards, and logical controls, which are built into software to authenticate users (through passwords or other means) and to restrict their access to certain data, programs, transactions, or commands. DOD policy states that access to automated information systems should be restricted based on one's need-to-know.

We found, however, that users were granted access to computer resources that exceeded what they required to carry out their job responsibilities, including sensitive system privileges for which they had no need. On one system, systems support personnel had the ability to change data in the system audit log. On three systems, we tested the accounts of 12 users having access to a command that would allow them to substitute an unauthorized data file for a legitimate file. Seven out of 12 did not have a need to use this command. We also found user accounts that had certain privileges—including sensitive security administration privileges— for which no evidence of authorization was available. Access authorization was poorly documented or undocumented for users at every site; management estimated that on one system more than 20,000 users were not authorized in writing.

Periodic review of user access privileges and monitoring of security violations and the use of powerful commands, utilities, and changes to sensitive files and records (such as user access profiles) are essential to preventing and detecting unauthorized activity. However, we found at every location we visited that there was inadequate periodic review of user access privileges to ensure that those privileges continued to be appropriate. Also, while the logging of security violations and access to

sensitive resources had improved, these audit logs were not being consistently reviewed. Similarly, we found that data processing customers were not updating users' access levels to reflect changes in their access requirements or to cancel the access of terminated employees.

Password management, though improved, was still weak in some areas. Users were not required to change their passwords often enough and in some cases were never required to change their passwords. Users were not prevented from using easily guessed passwords. These practices increase the risk that passwords will be guessed and systems will be compromised.

User accountability was also weakened by the use of generic (group) user accounts, wherein a single account is used by two or more users, contrary to DISA standards. In the case of one generic user account having system privileges, not only was the password known to multiple users, but it was neither encrypted in the system nor required to be changed periodically.

Application Software Development and Change Controls

Application software development and change controls prevent unauthorized programs or modifications to programs from being implemented to ensure that the software functions as intended. Program change control policies and procedures include review and approval of application change requests, independent review and testing of program changes, documentation of program changes, and formal authorization to implement those changes, along with the access controls necessary to ensure that these objectives are met.

We found that structured methodologies for designing, developing, and maintaining applications were inadequate or nonexistent. There was no requirement for users to document the planning and review of application changes and to test them to ensure that the system functioned as intended. Also, application programs were not adequately documented with a full description of the purpose and function of each module, which increases the risk that a developer making program changes will unknowingly subvert new or existing application controls.

One fundamental technique of program change control is the use of two or more computer processing environments to segregate the test and development versions of application programs and data from the production resources (those versions approved and currently being used by the data processing customer). We found that application programmers, users, and computer operators had direct access to production resources,

increasing the risk that unauthorized changes to production programs and data could be made and not detected. On one system, 74 user accounts had privileges enabling them to change program code without supervisory review and approval. This number had increased from the 37 users that we had documented in our earlier review. According to management, only four people should have this authority. On another system, nearly 300 programmers could alter production programs and data.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions without detection. As an example, a computer programmer should not be allowed to independently write, test, and approve program changes. In the information processing environment, the duties and access capabilities of systems programmers, application programmers, security administrators, and end-users, for example, should generally be segregated from one another.

Duties in the DOD computing environment were not adequately segregated. We found that personnel were still assigned both systems programming and security administration duties. These individuals could make unauthorized changes to programs and data while using their security privileges to disable the system's capability to create an audit trail of those changes. Thus they could, for example, modify payroll records or shipping records to generate unauthorized payments or to misdirect inventory shipments and suppress the related system audit data to avoid detection.

System Software

System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. Some system software can change data and program code without creating an audit trail or can be used to modify or delete audit trails.

Improperly configured or poorly maintained system software can be exploited to circumvent security controls to read, modify, or delete critical or sensitive data or programs. It can also be used to gain privileges to conduct unauthorized transactions or to circumvent edits or other controls built into application programs. For these reasons, system software vulnerabilities are a common target of hackers, both internal and external

to the entity. As a result, most entities have a separate set of procedures for controlling system software.

We found end-users had been given unnecessary (and in some cases unauthorized) access to system functions, tools, and data. For example, users could read system data files containing information useful to hackers. On four systems, users could view other users' output, which could include sensitive or confidential information. On one system, end-users had the capability to issue commands that would allow them to disrupt all processing on that system. As with other groups of users, the activities and access privileges of users with sensitive system privileges were not adequately monitored.

We also found system software maintenance issues which create security exposures. For example, we found system libraries for privileged programs (i.e., programs that are allowed to perform powerful system functions) that contained the names of nonexistent programs. By creating a new program with the same name as one of these nonexistent members, a user could install malicious code with the authority to make changes to the operating system, the security software, and user programs or data and to delete audit logs. We found that one site was running a proprietary mainframe operating system and other system software products that were no longer supported by the vendor. Management informed us that such software was needed to support application programs that had not yet been upgraded to run on a current version of the operating system. This site was also running programs that were undocumented. These practices increase the risk that security vulnerabilities or other problems will not be detected or corrected.

Service Continuity Controls

Service continuity controls ensure that when unexpected events occur, critical operations continue without undue interruption and critical and sensitive data are protected. A well-documented plan for disaster recovery and continuity of operations, based upon an up-to-date risk analysis and periodic testing, is critical to ensure that an organization can continue to fulfill its mission while responding to natural disasters, accidents, or other major and minor interruptions in data processing.

We found mission-related applications and the activities they support that are at risk because of inadequate planning for service continuity. Although DISA recommends nightly back-up of high-activity application data files, some information processing customers did not require that their application data be backed up frequently enough to ensure effective

mission support after a service disruption. This increases the risk that some data cannot be restored, particularly as temporary data files may not exist at the time the full system back-up is done, which is typically once a week. Also, although DISA requires that back-up tapes be stored at least 25 miles, and preferably 100 miles, from the processing site, we noted that one DMC was storing back-up tapes only 14 miles from the data center without having obtained a waiver from DISA. This increases the risk that both the back-up tapes and the data center could be affected by the same emergency.

We found that disaster recovery plans were incomplete and did not specify the order in which the customer's applications (or the programs within a particular application) should be restored. This increases the risk that relatively trivial functions may be restored before those that are most critical to the user's mission. One plan assumed the availability of hardware which was not on-site and was still in the procurement process.

Many DISA customers had not tested their recovery procedures or had not tested them under the conditions likely to prevail in the event of a disaster. These weaknesses increase the risk that the organization may fail in its mission or incur unnecessary expense as the result of a prolonged service interruption.

Progress in Addressing Security Weaknesses Varied Among DOD Organizations

Although each of the activities we evaluated had made some progress in addressing the individual weaknesses identified in our 1996 report, only DISA was implementing a comprehensive process for identifying, tracking, and resolving weaknesses within its jurisdiction. While implementation of this process was not yet complete, DISA had already identified and resolved thousands of specific control weaknesses.

In 1994, DISA created a task force to assess the security posture of its DMCs. This task force created an inspection checklist and a database to capture, track, and analyze its findings. The task force conducted system reviews and physical/environmental reviews, which have evolved into DISA's Security Readiness Review (SRR) process. DISA has steadily increased the number of security reviews performed. By the end of November 1998, DISA had completed 542 SRRs, generated a total of 14,860 findings, and reported that 11,418 of these findings had been corrected.

As DISA began implementing its SRR process, it also began drafting detailed technical guidance for individual systems, known as Security Technical Implementation Guides (STIG), which specify minimum standards for managing system software security. STIGs cover topics such as organizational relationships and responsibilities and the management processes and technical requirements needed to ensure hardware integrity, system software integrity, and data-level integrity. They define the requirements for interfacing the various components of system software and include such details as specific configuration options to be used, password management, testing requirements, and permissible levels of access to system resources. Most importantly, all DMC systems are subject to SRRs and DMC management is accountable for the findings generated. DISA officials and staff report that correcting SRR deficiencies is given a high priority because the status of SRR findings is a part of each DMC director's or commander's readiness report.

DISA has published STIGs for most of its systems and expects to have performed SRRs of all its systems before the end of 1999. Additional action, however, is needed to improve DISA's oversight of information security. For example, while the DISA inspector will generally verify any corrective action taken while he or she is still on-site, subsequent corrective actions are reported in the SRR database as having adequately addressed deficiencies even though the actions may not be verified until the next regularly scheduled inspection, which may be 15 to 36 months later. We found that this practice has resulted in some inaccuracies. We tested 55 deficiencies that were "accepted-as-fixed" in the SRR database and determined that about one-fourth had not been corrected. For example, several DMCs had reported that their system software configuration options had been changed to conform to DISA requirements, and the SRR database had been updated accordingly. However, our testing showed that the options in question were not in compliance with DISA standards. We did not attempt to determine whether these inconsistencies were the result of oversights, misrepresentations, or other factors. DISA officials agreed that more timely, independent verification of corrective actions is desirable and reported that they were exploring ways to address this issue.

Other DOD components had not made similar progress in instituting an effective oversight process. The modest improvements that these components had made were the result of individual and isolated command or unit actions rather than comprehensive service, agency, or department actions.

DOD Has Developed But Not Yet Implemented a Departmentwide Information Security Program

As stated in our executive guide on information security management,[12] a well-designed and well-managed information security program with senior-level support is essential for ensuring that an agency's controls are, and continue to be, appropriate and effective. The program should establish a process and assign responsibilities for systematically (1) assessing risk, (2) developing and implementing effective security policies and related control techniques, (3) promoting user awareness of security issues, (4) monitoring the appropriateness and effectiveness of these policies and techniques, and (5) providing feedback to managers who may then make needed adjustments. It should also establish a central management focal point for information security. This focal point functions as a facilitator and a conduit for information. It may also be a central resource for activities such as security training. Such a program can provide senior officials a means of managing information security risks and the related costs rather than just reacting to individual incidents.

In 1996, we reported that DOD lacked a departmentwide information security program to comprehensively address the general control weaknesses we had identified. We made a number of recommendations related to establishing such a program. DOD agreed with our recommendations and issued plans for the Defense-wide Information Assurance Program (DIAP), which is to provide the framework for a comprehensive information security program. It is too early to assess when, whether, or how effectively the provisions of the DIAP management and implementation plans will be implemented and coordinated with other related efforts or whether the DIAP will ultimately succeed in ensuring adequate information security throughout DOD.

Earlier Recommendations for Establishing a Departmentwide Information Security Program

The 10 recommendations in our September 1996 report to the Secretary of Defense, the DISA Director, and the CIOs of the military departments and other Defense agencies were aimed at

- empowering the DOD CIO to establish a comprehensive, departmentwide information security program;
- ensuring that security programs of the military departments and Defense agencies are consistent with the department program; and

[12]Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

- periodically reporting on progress in improving controls over information security.

DOD concurred with these recommendations and committed to resolving the issues and implementing the recommendations. The department has reported that corrective actions are in progress for each of these recommendations. The full text of the recommendations appears in appendix I.

Departmentwide Information Security Program Being Developed

At the time of our current review, DOD was developing but had not yet implemented a departmentwide security program in response to the recommendations in our earlier reports. On January 30, 1998, the Deputy Secretary of Defense approved the Defense-wide Information Assurance Program (DIAP) and distributed a DIAP management plan to senior DOD officials. The Implementation Plan for the DIAP, which was finalized on February 12, 1999, describes at a high level the program's goals, objectives, and organizational structure. DIAP staff will be responsible for creating a DIAP concept of operations to address the program's operational structure and processes. The program is still being staffed.

The DIAP integrates component information assurance (IA) activities into a single program under the DOD CIO, combining centralized oversight with decentralized execution. The DIAP staff will carry out the planning, programming, budgeting, and review of all IA activities throughout DOD. All IA investments and expenditures will be reported as part of the DIAP budget beginning in fiscal year 2000. DOD components will be responsible for carrying out their portions of the DIAP annual plan and for reporting on their activities to the Director of Information Assurance, who in turn reports to the DOD CIO.

DIAP planning documents, which incorporate at a high level most of the best practices associated with successful information security management, indicate that DOD recognizes and is attempting to establish the departmentwide management structure needed to manage the complex information security risks associated with its heavy reliance on interconnected computer systems. For example, because the DIAP is an integrated program under the DOD CIO, it provides a central focal point for identifying risks affecting multiple Defense components and coordinating the selection, funding, and implementation of appropriate mitigating controls.

The DIAP also establishes a Senior DIAP Steering Group composed of representatives from the services, Joint Staff, National Security Agency, and DISA. Thus, it involves senior management officials responsible for mission-related operations and assets as well as technical security specialists to help ensure that the related information security risks are fully understood and that an appropriate level of resources is provided to mitigate them.

DIAP plans call for development of performance measures and an annual IA operational assessment, both prerequisites for effective feedback and reporting. They also call for an annual review of DIAP goals and related service and Defense agency plans, which is important to identify new risks, threats, and countermeasures to ensure that controls remain appropriate and effective. As DOD develops operating policies and procedures to support the DIAP, it can draw upon the existing information security guidance and best practices being used by other organizations, which define basic elements needed to provide effective feedback on information security controls. For example, our Federal Information System Controls Audit Manual defines information system control objectives and provides a framework for assessing the effectiveness of those controls. Similarly, DISA's SRR and STIG compliance process provides a model for testing to determine if controls are functioning as intended, monitoring compliance, and tracking and reporting weaknesses identified during testing for resolution and review by senior management.

In December 1998, a newly-created Joint Task Force for Computer Network Defense began coordinating and directing the defense of DOD computer systems and networks against strategic attack. Its functions include (1) situation monitoring and assessment, (2) directing DOD actions to stop attacks, contain damage, restore functionality, and provide feedback to users, (3) coordinating DOD defensive actions with other government agencies and private organizations as appropriate, (4) participation in joint training exercises, and (5) development of contingency plans and techniques.

The Joint Task Force supports the DIAP by providing the monitoring tools to identify hostile attacks to DOD systems through its networks. However, the DIAP does not yet adequately address the vulnerabilities that make such attacks possible or the threats to information security that cannot be detected through network monitoring. The latter include (1) environmental threats, such as natural disasters or accidents, (2) the unauthorized activities (such as espionage, sabotage, or embezzlement) of

authorized users, programmers, or terminated employees who still have system access due to lax security management, and (3) data loss or corruption following a service interruption, due to poor back-up and contingency planning.

DOD believes the DIAP and task force initiatives will address the computer control weaknesses noted in our previous reports and our current review. However, it is too early to determine how the provisions in the DIAP plans will be implemented or how the Joint Task Force and other operational efforts yet to be developed will be coordinated with it. Thus, we were unable to assess whether these efforts will ultimately be successful in ensuring adequate information security throughout DOD. We will monitor the implementation of the DIAP as part of our oversight of DOD information security.

Conclusions

Departmentwide, DOD has made limited progress in correcting the general control weaknesses we reported in 1996. As a result, these weaknesses persist across every area of general controls. However, DISA has developed technical standards and is implementing a Security Readiness Review process that provides a model for information security management throughout its DMCs. DISA has not fully implemented this information security program and still needs to address certain shortcomings. Specifically, the quality of data in its SRR database could be improved through more timely independent verification of corrective actions by the DMCs or other parties.

The DIAP implementation plan provides the framework for a departmentwide information security program. However, because DOD has not yet implemented DIAP, we cannot yet determine whether it will ultimately succeed in ensuring adequate security throughout the department. Close coordination between the DIAP, the Joint Task Force, and other operational efforts will be crucial to comprehensively addressing DOD's information security weaknesses. DISA's program and other models for information security management offer approaches that DOD could adapt and integrate into its departmentwide program.

Recommendations

In addition to reaffirming the recommendations in our 1996 reports, we recommend that, to realize the full potential and maximize the

effectiveness of DISA's security oversight program, the DIAP, and other DOD IA initiatives, the Secretary of Defense take the following actions.

- Direct the DISA Director to expand the Security Readiness Review process to include timely and independent verification of the corrective actions reported by DMCs or other responsible parties.
- Direct the DOD CIO to ensure that the Defense-wide Information Assurance Program defines how its efforts will be coordinated with the Joint Task Force and other related initiatives.

Agency Comments and Our Evaluation

DOD officials generally concurred with the report and our recommendations, noting that this report adds credence to efforts to heighten awareness within the DOD community of the serious risks that accompany poor security practices in information systems. They stated that the department is actively working to correct the deficiencies cited in the report and that they believe it is making progress in reducing the risks to its information systems. They also noted that the task is large and many corrective actions are underway, and affirmed that the continued development of the DIAP and other efforts will strengthen the department's information security posture.

With regard to our recommendation concerning DISA's verification of corrective actions, DOD officials acknowledged problems with the accuracy of reported fixes at Defense Megacenters. They advised us that DISA has since modified its procedures to include a specific check of the validity of entries made on previously documented Security Readiness Reviews. According to DISA, the revised procedures call for incorrect entries and repeat findings to be noted as serious concerns to DMC facility directors.

Regarding our recommendation concerning coordination of the DIAP with the Joint Task Force and related initiatives, DOD officials affirmed that the DIAP and other initiatives in the department—such as the Joint Task Force for Computer Network Defense (JTF-CND)—will address the computer control weaknesses cited in our report and recognized that efforts must be coordinated between the DIAP and those other initiatives. They pointed out that the DIAP has established close working relationships with the military services, agencies, Joint Staff, and other elements within DOD, including the newly established JTF-CND. They noted that an implementation plan is being prepared that aligns JTF-CND under the

Commander-in-Chief, United States Space Command, and that the DIAP has participated in the working groups to create this plan.

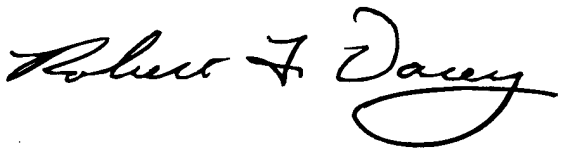
Lastly, they referred to two other DOD initiatives assessing (1) the threat to information systems posed by insiders and (2) the training of DOD information technology employees. They noted that these studies are expected to result in recommendations related to the training of system administrators and the controls over their access to information systems that, when implemented, should yield significant improvements to the security of DOD information systems.

This report contains recommendations to you. The head of a federal agency is required by 31 U. S. C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Reform within 60 days of the date of this report. You must also send a written statement to the House and Senate Committees on Appropriations with the agencies' first request for appropriations made over 60 days after the date of this report.

We are sending copies of this report to Senator Fred Thompson, Senator Joseph Lieberman, Representative Floyd Spence, Representative Ike Skelton, Representative Dan Burton, Representative Henry A. Waxman, Representative C.W. Bill Young, and Representative John P. Murtha in their capacities as Chair or Ranking Minority Member of Senate and House Committees and Subcommittees. We are also sending copies of this report to Mr. Arthur L. Money, Senior Civilian Official for the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and DOD Chief Information Officer, and Lieutenant General David J. Kelley, Director, Defense Information Systems Agency. Copies will also be made available to others upon request.

If you or your office have any questions concerning this report, please contact me or Les Thompson, Assistant Director, at (202) 512-3789. Individuals making key contributions to this report are listed in appendix II.

Sincerely yours,



Robert F. Dacey
Director, Consolidated Audit and Computer
Security Issues

Contents

Abbreviations

CDA	Central Design Activity
CIO	Chief Information Officer
DFAS	Defense Finance and Accounting Service
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DMC	Defense Megacenter
DOD	Department of Defense
IA	information assurance
JTF-CND	Joint Task Force for Computer Network Defense
SA	Security Administor
SRR	Security Readiness Review
STIG	Security Technical Implementation Guide

Recommendations Made in GAO/AIMD-96-144

DOD has reported that corrective actions are in progress for each of the recommendations below. While none are fully completed, DOD believes that its corrective actions will address all of our recommendations, primarily through the DIAP. As noted in this report, it is too early to determine how the provisions in the DIAP will be implemented and, thus, whether these corrective actions will effectively address our recommendations.

I	We recommend that the Secretary of Defense assign clear responsibility and accountability within the Office of the Secretary of Defense, the military services, and the Defense agencies for ensuring the successful implementation of an information security program that includes, for example, departmentwide policies for preventing, detecting, and responding to hacker attacks on Defense information systems.
II	We further recommend that you direct the DOD CIO to develop and implement a comprehensive DOD-wide computer security management program that includes the hacker prevention policies we previously recommended as well as • establishing a risk-based control program to assess computer security in DOD computer systems, • developing and implementing effective security policies and related control techniques, and • reporting to DOD managers on security issues impacting their information processing systems.
III	We also recommend that you direct the Deputy Secretary of Defense to ensure that the duties established for the military departments' and Defense agencies' CIOs include reporting on ongoing computer security efforts and activities to the DOD CIO for review, assessment, and appropriate action to ensure proper coordination and an integrated information technology structure within the Department.
IV	Further, you should direct the DOD CIO to review and assess the specific deficiencies noted and establish a process to address them.
V	In addition, we recommend that the DISA Director, the CIOs of the military departments, and the CIOs of the other Defense agencies submit their policies and procedures to improve general computer controls to the DOD CIO for review, assessment, and appropriate action to ensure a comprehensive security approach is operational throughout the Department. Such policies and procedures should • limit computer system access authorizations to only those who need access to perform their work responsibilities, and are periodically reviewed to ensure their continued need; • require sensitive data files and critical production programs to be identified and successful and unsuccessful access to them to be monitored; • strengthen security software standards in critical areas, such as by preventing the reuse of passwords and ensuring that security software is implemented and maintained in accordance with the standards; • control physical security at computer facilities; and • provide for completing and testing disaster recovery plans.

VI	To ensure that general computer controls are improved at the DMCs, we recommend that the DOD CIO direct the DISA Director to develop and implement a comprehensive computer security program at the DMCs, consistent with the DOD-wide program, that includes the elements outlined in this report. These elements encompass • policies and procedures to ensure that access to DMC computer facilities is appropriately granted and periodically reviewed, • clearly defined roles and responsibilities of DMC employees, information system security officers, and security managers, and • security oversight at each DMC to monitor, measure, test, and report on the ongoing effectiveness of computer system, network, and process controls.
VII	In addition, we recommend that the CIOs of the military departments and the Defense agencies submit plans for coordinating with DISA to improve computer controls affecting DMC operations to the DOD CIO for review, assessment, and appropriate actions. Greater cooperation is necessary, for example, to • determine who is given access to computer systems applications, • identify critical computer systems applications to be covered by disaster recovery plans, and • ensure that locally designed software application program changes are in accordance with prescribed policies and procedures.
VIII	Also, the DISA Director and the CIOs of the military departments and Defense agencies should provide their plans to the DOD CIO, for review, assessment, and appropriate action to ensure that computer system security reviews are performed as part of future transfers of computer systems to the DMCs.
IX	Further, the DOD CIO should monitor implementation of those plans.
X	Finally, to strengthen DOD's computer security program in a coordinated and timely manner, we recommend that you • direct the DOD CIO to monitor and to periodically report on the status of the actions taken to improve computer security throughout DOD and • ensure that the DOD CIO has the necessary authority to ensure that there are adequate computer security controls throughout DOD, including the military departments and Defense agencies.

Appendix II

GAO Contacts and Staff Acknowledgements

GAO Contacts

C. Les Thompson, (202) 512-3789
Robert F. Dacey, (202) 512-3317

Acknowledgments

In addition to those named above, Sharon Kittrell, Jean Boltz, Edward Glagola, Linda Sellevaag, Gary Austin, and Walter Opaska made key contributions to this report.

Related GAO Products

Major Management Challenges and Program Risks: Department of Defense (GAO/OCG-99-4, January 1999).

Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets (GAO/T-AIMD-98-312, September 23, 1998).

Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls (GAO/T-AIMD-98-308, September 28, 1998).

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998).

Defense Computers: Year 2000 Computer Problems Put Navy Operations at Risk (GAO/AIMD-98-150, June 30, 1998).

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998).

Executive Guide: Information Security Management: Learning From Leading Organizations (GAO/AIMD-96-68, May 1998).

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

Department of Defense: Financial Audits Highlight Continuing Challenges to Correct Serious Financial Management Problems (GAO/T-AIMD/NSIAD-98-158, April 16, 1998).

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

Federal Management Issues (GAO/OCG-98-1R, January 9, 1998).

Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk (GAO/AIMD-98-5, October 20, 1997).

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997).

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997).

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997).

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997).

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997).

Defense Financial Management: Immature Software Development Processes at Indianapolis Increase Risk (GAO/AIMD-97-41, June 6, 1997).

Defense IRM: Investments at Risk for DOD Computer Centers (GAO/AIMD-97-39, April 4, 1997).

High-Risk Series: Defense Financial Management (GAO/HR-97-3, February 1, 1997).

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1, 1997).

Financial Management: DOD Inventory of Financial Management Systems Is Incomplete (GAO/AIMD-97-29, January 31, 1997).

Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996).

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996).

Defense Industrial Security: Weaknesses in U.S. Security Arrangements With Foreign-Owned Defense Contractors (GAO/NSIAD-96-64, February 20, 1996).

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER